IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CRIMINAL NO. 2:16cr36**
	)	
GERALD ANDREW DARBY,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S SECOND MOTION TO SUPPRESS

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, Elizabeth M. Yusi, Assistant United States Attorney, and Leslie Williams Fisher, United States Department of Justice Trial Attorney, and submits its response in opposition to the defendant GERALD ANDREW DARBY's Second Motion to Suppress information identifying his home computer recovered pursuant to a search warrant that authorized the use of a network investigative technique to recover such information. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

After a months-long investigation, the Federal Bureau of Investigation (FBI) briefly assumed administrative control of "Playpen", a website dedicated to the sharing of child pornography. The FBI also sought and obtained a warrant from a magistrate judge in the Eastern District of Virginia permitting it to deploy a "Network Investigative Technique" (the "NIT") during that same period, which would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed Internet Protocol (IP) address. The server on which the NIT was deployed was located in the Eastern District of Virginia. The deployment of the NIT also occurred within the Eastern District of Virginia.

Among the IP addresses identified accessing Playpen was one associated with defendant Gerald Andrew Darby ("the defendant"). Following the execution of a search warrant at the defendant's home in Suffolk, Virginia, located within the Eastern District of Virginia, the defendant was indicted and arrested on charges of receipt and possession of child pornography involving a prepubescent minor. Defendant's First Motion to Suppress was filed on April 13, 2016 (Doc. 15) and the Government's Response to Defendant's First Motion to Suppress was filed on April 27, 2016 (Doc. 16). The defendant has now filed a second motion to suppress. He continues to seek to suppress the information obtained by the NIT used to identify his home computer and its location, along with all other evidence derived from that information. For the reasons that follow, his motion should be denied.

The United States incorporates and respectfully refers this Court to Government's Response to Defendant's First Motion to Suppress (Doc. 16) for a more detailed factual background of the investigation, the Tor network, and the Playpen website.

ARGUMENT

I. The Magistrate Judge Had Jurisdiction to Issue the NIT Warrant as Applied to the Defendant

The defendant argues two things: (1) the issuance of the NIT warrant violated Rule 41 of the Federal Rules of Criminal Procedure, and (2) Section 636(a) of the Federal Magistrates Act puts territorial limits on the geographic areas in which a magistrate judge has jurisdiction to issue warrants. The defendant is wrong on both arguments.

First, Rule 41 authorizes a magistrate judge with authority in the district to issue a warrant to search for and seize a person or property located within the district. Fed. R. Crim. P. 41(b)(1). In this case, that is precisely what occurred. There is no doubt that the magistrate who

issued the initial warrant authorizing the NIT had clear authority to do so pursuant to Rule 41(b) as applied to the defendant in this case.

Second, a magistrate judge for the Eastern District of Virginia authorized the warrant for the NIT to be deployed on a server located in the Eastern District of Virginia. The defendant, at all times relevant to the charges against him, was also located in the Eastern District of Virginia. The information obtained from that NIT, specifically an IP address registered to the defendant, led law enforcement to obtain a search warrant for the defendant's home. Defendant's home is located in Suffolk, Virginia, within the Eastern District of Virginia. Based on even the narrowest plain reading of the Federal Magistrates Act, there is no doubt that the magistrate who issued the NIT warrant had authority to issue such warrant as applied to the defendant. The defendant can make no plausible argument that the magistrate who issued the NIT warrant did not have jurisdiction to issue the warrant as it applied to him, nor can he possibly show any prejudice resulting from that application.

A. The Issuance Of The NIT Warrant Does Not Violate Rule 41

Even assuming, *arguendo*, that the magistrate who issued the NIT warrant was in a different judicial district than the defendant's residence, the issuance of the NIT warrant does not violate Rule 41. In fact, three separate provisions of Rule 41(b) support issuance of the NIT warrant.

First, Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the warrant authorized use of the NIT (a set of computer instructions) located on a server in the Eastern District of Virginia when the warrant was issued. As Rule 41(a)(2)(A) defines "property"

to include both "tangible objects" and "information," the NIT constituted property located in the Eastern District of Virginia when the warrant was issued. Moreover, the NIT was deployed only to registered users of Playpen who logged into the website, located in the Eastern District of Virginia, with a username and password. Each of those users—including the defendant—accordingly reached into the Eastern District of Virginia's jurisdiction to access the site (and the child pornography therein). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT even outside of the Eastern District of Virginia.

Second, Rule 41(b)(4) specifies that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install a tracking device in a container holding contraband, and investigators might then determine the location of the container after targets of the investigation carry the container outside the district. In this case, the NIT functioned in a similar manner, except in the Internet context. Investigators installed the NIT in the Eastern District of Virginia on the server that hosted Playpen. When the defendant logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information from the defendant's computer back to law enforcement. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate the defendant. Thus, even if Rule 41(b)(2) did not provide authority to issue the warrant, Rule 41(b)(4) did so.

Finally, the NIT warrant was issued by a judge in the district with the strongest known connection to the search: the defendant entered the Eastern District of Virginia by accessing the Playpen server there, retrieved the NIT from that server, and the NIT sent his network information back to a server in that district. The magistrate judge had authority under Rule 41(b)(1) to authorize a search warrant for "property located within the district." The use of the Tor hidden service by the defendant and other Playpen users made it impossible for investigators to know in what other districts, if any, the execution of the warrant would take place. In this circumstance, it was reasonable for the Eastern District of Virginia magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the NIT warrant does not risk significant abuse because, as with all warrants, the manner of execution "is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

The defendant cites a magistrate judge's opinion holding that Rule 41(b) does not authorize issuance of a warrant for use of a different (and significantly more invasive) NIT than the one used in this case. *See In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp.2d 753 (S.D. Tex. 2013). *In Re Warrant*, though, does not undermine the magistrate judge's decision to issue the warrant here. The reasoning of the Texas magistrate judge's decision does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp.2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply because there was no showing that the installation of the NIT software would be within its district. *See id.* That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the server in the Eastern District of Virginia. As the analogy to physical tracking devices demonstrates, the

government "installs" the NIT within the meaning of Rule 41(b)(4) when it adds the NIT to computer code on a computer in the issuing court's district. The defendant's subsequent retrieval of the NIT and its collection of information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included "installation" on the defendant's computer.

In support of his claims that the NIT warrant violates Rule 41, the defendant points to an amendment to Rule 41 that the government proposed in 2013 and a memorandum regarding that proposed amendment written in 2014. On April 28, 2016, the Supreme Court ordered that the amendment be incorporated into Rule 41 and take effect on December 1, 2016. (*See* Ex. 1). The proposed amendment to Rule 41 was designed to clarify that courts have venue to issue a warrant "to use remote access to search electronic media storage" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." This proposed amendment and the accompanying letter from the then Assistant Attorney General for the Criminal Division of the Department of Justice and the 2014 memorandum do not support the conclusion that the actions in this case violate Rule 41. As the 2014 memorandum states, the proposed amendment is meant only to clarify Rule 41, and would not authorize the government to undertake an search or seizure, or use any remote search technique not already permitted under current law. That the Department of Justice seeks greater clarity in the rule does not convert conduct taken in good faith to a deliberate and intentional violation of the rule.

B. The Issuance of The NIT Warrant Does Not Violate The Federal Magistrates Act

Even assuming, *arguendo*, that the magistrate judge who issued the NIT warrant was in a different judicial district than the defendant's residence, the issuance of the NIT warrant does not violate the Federal Magistrates Act, 28 U.S.C. 636. Section 636(a) provides in relevant part:

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where the court may function, and elsewhere as authorized by law—
>
> (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts[.]"

28 U.S.C. 636(a).

Reading the plain language of the statute, Section 636(a) limits where a magistrate may *possess* his powers, but not where those powers can have *effect.* Therefore a warrant must issue from a district described in Section 636(a) (for example, the district in which the magistrate judge sits), but not that the warrant's effects must be limited to that district. Rule 41(b) supports this reading that a magistrate can possess a power that has effects beyond the places described in Section 636(a). For example, Rule 41(b)(2) provides that "a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district" so long as the property is located within the district when the warrant is issued.

None of the case law defendant relies on to support his argument that the issuance of the NIT warrant violated the Federal Magistrates Act: a decision out of the District of Massachusetts, *United States v. Levin,* Crim. No. 15-10271, 2016 WL 1589824 (D. Mass. Apr. 20, 2016), a decision out of the District of Oklahoma in *United States v. Arterbury,*

Crim. No. 15-182, ECF No. 42 (D. Okla. Apr. 25, 2016), and the concurring opinion in the Tenth Circuit case *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015).

None of these cases are persuasive or precedential here. Judge Gorsuch's concurring opinion in *Krueger* states that Section 636(a) puts territorial limits on the "geographic areas in which a federal magistrate judge's powers are effective." Not only is a concurring opinion from another circuit not precedent for this Court, but, for the reasons stated above, is an incorrect reading of Section 636(a). Furthermore, the facts in *Krueger* are easily distinguishable from the facts here. In *Krueger,* a magistrate judge in Kansas issued a search warrant for physical property known to be located in Oklahoma. In the instant case, a magistrate judge issued a warrant allowing a NIT to be deployed on a server located within her own district. Finally, again, the reasoning in *Krueger* does not apply to this case, because the defendant here was located in the same district as the magistrate who issued the NIT warrant.

Likewise, neither a district court decision out of Massachusetts nor Oklahoma is precedent for this Court. While the government does not concede that the decisions in *Levin* and *Arterbury* were correct, they are again not relevant in this case. The courts in *Levin* and *Arterbury* analyzed the application of the NIT warrant on defendants found outside of the Eastern District of Virginia. Here, the defendant was found in the same district as the magistrate who issued the NIT warrant.

II. The Defendant Lacks Standing to Raise the Argument That the Magistrate Judge Lacked Jurisdiction Outside the Eastern District of Virginia.

The defendant lacks standing to make any argument regarding how the issuance of the NIT warrant would apply to a third party found outside of the Eastern District of Virginia. While the government does not concede that the issuance of the NIT warrant exceeded the magistrate's

authority even as applied to a subject found outside of the Eastern District of Virginia, the defendant here does not have standing to even raise that argument. The defendant is located in the Eastern District of Virginia. The magistrate who issued the NIT warrant was located in the Eastern District of Virginia.

The Fourth Amendment affords individuals the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. However, the scope of that right is limited. It depends on "whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 142 (1978). A person who seeks to suppress "damaging evidence secured by a search of a third person's premises or property" in which he has no cognizable privacy interest "has not had any of his Fourth Amendment rights infringed" and is therefore not entitled to benefit from the exclusionary rule's protections. *Rakas*, 439 U.S. at 134.

The defendant has no privacy interest in any property found as a result of the NIT warrant that is not his own property, and therefore no standing to raise the argument that the magistrate lacked jurisdiction to issue the warrant as applied to individuals outside the Eastern District of Virginia.

III. The NIT Warrant was Reasonable Under the Fourth Amendment

Even if the defendant were correct that the warrant did not fit within the letter of Rule 41(b), the use of the NIT would nevertheless still be reasonable under the Fourth Amendment. The Supreme Court has recognized that the presumption that warrantless searches are unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law

enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). Courts must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 59 (2013). Some of the factors relevant in determining whether exigent circumstances exist in a particular case include the degree of urgency involved and the amount of time necessary to obtain a warrant, law enforcement's reasonable belief that the contraband is about to be removed or destroyed, the possibility of danger to police guarding the site, information indicating the possessors of the contraband are aware that the police are on their trail, and the ready destructibility of the contraband. *United States v. Turner*, 650 F.2d 526, 528 (4th Cir. 1981)(citing *United States v. Rubin*, 474 F.2d 262, 268 (3d Cir. 1973)).

Here, even if the government could not obtain a warrant for use of the NIT that complied with the letter of Rule 41(b), ample exigent circumstances existed to justify its use. Playpen enabled ongoing sexual abuse and exploitation of children, and deploying the NIT against Playpen users was necessary to stop the abuse and exploitation and to identify and apprehend the abusers. As of early January of 2016, use of the NIT in this investigation had led to the identification or recovery from abuse of twenty-six child victims. (*See* Ex. 2). The FBI also has identified at least thirty-five individuals who have been determined to be "hands on" child sexual offenders, and seventeen individuals who have been determined to be producers of child pornography. Id.

The information the NIT collected was also fleeting. If law enforcement had not collected IP address information at the time of user communications with Playpen, then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Accordingly, if the warrant could not have been issued, then no warrant could have been

obtained in a reasonable amount of time to identify perpetrators. See *United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. As thoroughly explained in the Government's Response to Defendant's First Motion to Suppress, the defendant does not have a reasonable expectation of privacy in his IP address. (Doc. 16 at 33-34).

In sum, the NIT warrant provided authority for use of the NIT, and it is certainly preferable that the government obtain warrants (as it did here) to investigate large criminal enterprises like Playpen. Criminals' use of anonymizing technologies like Tor to perpetrate crimes should not place them beyond the reach of law enforcement (or courts). But even if no court had authority to issue a warrant to deploy a NIT to investigate Playpen users outside the Eastern District of Virginia, as the defendant essentially argues is the case, its use was nonetheless reasonable under the Fourth Amendment.

IV. Suppression is Not Mandatory

Additionally, as previously argued in the Government's Response to the Defendant's First Motion to Suppress (Doc. 16), even if the NIT warrant does not satisfy the Fourth Amendment, the good faith exception bars suppression here. The NIT warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. The issuing magistrate judge did not abandon her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. The affidavit made

a strong, comprehensive showing of probable cause to deploy the NIT. Therefore, the agents' reliance on the magistrate judge's authority to issue the warrant was objectively reasonable.

CONCLUSION

For the foregoing reasons, the defendant's Second Motion to Suppress the information identifying his home computer recovered pursuant to a search warrant that authorized the use of the network investigative technique should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By: _____/s/_____

Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov

Leslie Fisher
Trial Attorney
U.S. Department of Justice, Criminal Division
Child Exploitation & Obscenity Section
1400 New York Ave. NW, Suite 600
Washington, D.C. 20005
Office: (202) 616-2557
Fax: (202) 514-1793
Leslie.fisher2@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 9th day of May, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Rodolfo Cejas
Assistant Federal Public Defender

_____/s/_____
Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov